Basi algebriche dell'algoritmo RSA

VR, Feb. 2013

$\boxed{\text{messaggio } x} \xrightarrow{\text{criptazione}} \boxed{\text{messaggio cifrato } y} \xrightarrow{\text{trasmissione}} \boxed{y} \xrightarrow{\text{decriptazione}} \boxed{x}$

Crittografia a chiave pubblica
procedura asimmetrica
- chiave pubblica criptazione (facile da produrre)
- chiave privata decriptazione praticamente impossibile risalire dalla chiave pubblica

- Un tempo crittografia principalmente per scopi militari, si concordavano chiavi segrete per scambiarsi messaggi
- Oggigiorno esigenza cifrare dati quotidianamente (banca, Internet)
- serve procedura più semplice e veloce
- l'utente riceve chiave di criptaz. al momento della transazione, da cui non può risalire alla chiave decript.

può essere anche il contrario (firma elettronica: in tal caso l'utente invia x, y e la chiave di decriptazione)

Rivest – Shamir – Adleman (1977) MIT
- facile produrre numeri primi grandi p, q e calcolare $n = pq$
- praticamente impossibile da n risalire a p, q

tempo di fattorizzazione con i mezzi attuali è troppo lungo, basta cambiare p, q di tanto in tanto

"one-way function"
biiettiva, ma non è possibile ricavare l'inversa

L'algoritmo RSA:

L'algoritmo base (può essere combinato col Teorema Cinese dei Resti ecc.)

Dati p, q primi grandi, almeno 300 cifre
- poniamo $n = pq$
  $m = (p-1)(q-1)$
- scegliamo $1 < a < m$ che sia primo con m
- calcoliamo $1 < b < m$ tale che $ab = 1 + \beta m$ con $\beta \in \mathbb{N}$

Messaggio: $1 < x < \min(p,q) < n$

testo $\xrightarrow{\text{ASCII}}$ una sequenza di numeri di una certa lunghezza tale che $< \min(p,q)$

$\boxed{x} \xrightarrow[(a,n)]{} \boxed{y} \longrightarrow \boxed{y} \xrightarrow[(b,n)]{} \boxed{x'}$

Criptazione: $y \in \{1, \dots, n-1\}$
è il resto della divisione di x^a per n
$$x^a = nq + y \quad \text{con } q \in \mathbb{Z}$$
Chiave di criptazione: (a, n)

Decriptazione: $x' \in \{1, \dots, n-1\}$
è il resto della divisione di y^b per n
$$y^b = nq' + x' \quad \text{con } q' \in \mathbb{Z}$$
Chiave di decriptazione: (b, n)

$x^a \equiv y \bmod n$
$y^b \equiv x' \bmod n$

Si verifica $\boxed{x' = x.}$

non si può risalire dall'una all'altra senza conoscere p, q

ESEMPIO $p=3,\ q=11 \Rightarrow n=33\ ,\ m=20$

scegliamo $a=7$

Calcoliamo b:

$$3\cdot 7 = 1+20 \Rightarrow b=3$$

Algoritmo Euclideo: $1=MCD(20,7)$ attraverso divisioni succ. espresso come comb. lin. di 20 e 7

$$20 = 2\cdot 7 + 6$$
$$7 = 1\cdot 6 + 1$$

quindi $1 = 7-6 = 7-(20-2\cdot 7)$
$= 3\cdot 7 - 20$

Messaggio $x=2$:

$$x^a = 2^7 = 128 = 3\cdot 33 + 29 \Rightarrow y=29$$
$$y^b = 29^3 = 24389 = 739\cdot 33 + 2 \Rightarrow x'=2.$$

Perché funziona?

§1 L'anello $\mathbb{Z}/n\mathbb{Z}$

§2 Un po' di teoria di gruppi

§3 Dimostrazione

§1 L'anello $\mathbb{Z}/n\mathbb{Z}$

Sia $n \in \mathbb{N}$, $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$

Definiamo una relazione su $\mathbb{Z}$:

$$a \sim b \quad \text{se} \quad a - b \in n\mathbb{Z}$$

Osservazioni:

(1) $a \sim b \iff a$ e b danno lo stesso resto divisi per n

$\iff a \equiv b \mod n$

(2) $\sim$ è una relazione di equivalenza su $\mathbb{Z}$:

riflessiva, simmetrica, transitiva: $a \sim b$ e $b \sim c \Rightarrow a-b, b-c \in n\mathbb{Z}$

$\Rightarrow a - c = (a-b) + (b-c) \in n\mathbb{Z} \Rightarrow a \sim c$

(3) La classe di equivalenza di a è la classe di resto

$\overline{a} = \{x \in \mathbb{Z} \mid x \sim a\} = \{nq + a \mid q \in \mathbb{Z}\}$ di a modulo n

(4) $a \sim b \iff \overline{a} = \overline{b} \iff \overline{a} \cap \overline{b} \neq \emptyset$

vero per qualsiasi relaz. di equiv.

$x \in \overline{a} \Rightarrow x \sim a \underset{\text{trans}}{\Rightarrow} x \sim b$

$\Downarrow$

$\exists\, x \sim a$ e $x \sim b$ $\underset{\text{trans simm.}}{\Rightarrow} a \sim b$

quindi due classi di equiv. distinte sono disgiunte!

(5) $\sim$ induce una partizione su $\mathbb{Z}$

$$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \dots \cup \overline{n-1}$$

per $n=2$

$\mathbb{Z} = \{\text{pari}\} \cup \{\text{dispari}\}$

Poniamo $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$ l'insieme delle classi di resto modulo n

sono insiemi, li vediamo come elementi

Definiamo due operazioni su $\mathbb{Z}/n\mathbb{Z}$: dati $a, b \in \mathbb{Z}$, poniamo

$$\overline{a} + \overline{b} = \overline{a+b}$$

$$\overline{a} \cdot \overline{b} = \overline{ab}$$

Esempio! per $n=6$: $\overline{2} = \overline{8} = \overline{14} = \dots$ ad es.

Ben definite: (indipendenti dalla scelta del rappresentante a, b)

per $\cdot$ (per $+$ più facile)

se $\overline{a} = \overline{a'}$, $\overline{b} = \overline{b'}$, allora $a - a' \in n\mathbb{Z}$ e $b - b' \in n\mathbb{Z}$,

quindi $ab - a'b' = ab - a'b + a'b - a'b' =$

$= (a-a')b + a'(b-b') \in n\mathbb{Z}$, e perciò $\overline{ab} = \overline{a'b'}$

<u>Esempio</u>: $n=6$ $\quad \overline{3}+\overline{5}=\overline{2}$ $\qquad \mathbb{Z}/6\mathbb{Z}=\{\overline{0},\overline{1},\dots,\overline{5}\}$

$$\overline{2}+\overline{4}=\overline{0}$$

$$\overline{2}\cdot\overline{5} \quad \cancel{\overline{2}}\cdot\cancel{\overline{4}} = \cancel{\overline{2}}\ \overline{4}$$

$$\overline{2}\cdot\overline{3}=\overline{0} \quad \Rightarrow \quad \overline{2},\overline{3} \text{ non invertibili}$$

$$\overline{5}\cdot\overline{5}=\overline{1}$$

PAUSA

$(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ è un anello

- gruppo abeliano rispetto a +
- proprietà associativa
- commutativo, elemento neutro rispetto a $\cdot$
- leggi distributive

$\overline{0}$ elemento neutro di +

$\overline{1}$ elemento neutro di $\cdot$

Elementi invertibili rispetto a $\cdot$ (vedi sopra ↑)

$$\overline{a}\cdot\overline{b}=\overline{1} \iff 1-ab\in n\mathbb{Z}$$

$$\iff 1=ab+nq \quad \text{con } q\in\mathbb{Z}$$

identità di Bézout

$$\iff a,n \text{ sono coprimi}$$

"$\Longrightarrow$" se p fosse divisore comune, si avrebbe $p/1$ ↯

"$\Longleftarrow$" se a,n coprimi, si calcola $1=MCD(a,n)$ con l'Algoritmo Euclideo e risalendo si trovano b,q (vedi Esempio)

Quindi $\overline{a}\in\mathbb{Z}/n\mathbb{Z}$ invertibile $\iff$ a primo con n.

L'insieme degli elementi invertibili

$$\mathbb{Z}/n\mathbb{Z}^* = \{\overline{a}\in\mathbb{Z}/n\mathbb{Z} \mid 1\le a\le n-1 \text{ con } MCD(a,n)=1\}$$

$\varphi(ab)=\varphi(a)\varphi(b)$

è un gruppo rispetto a $\cdot$ con elemento neutro $\overline{1}$

Il suo ordine è dato dalla <u>funzione di Eulero</u> $\varphi: \mathbb{N}\to\mathbb{N}$, dove $\varphi(n)$ è il numero degli $1\le a\le n-1$ primi con n.

x coprimo con $ab \iff$ coprimo con a e con b

Si ha $\varphi(p)=p-1$ se p è primo, $\varphi(6)=2$, $\varphi(pq)=(p-1)(q-1)$.

$\mathbb{Z}/a\mathbb{Z}\times\mathbb{Z}/b\mathbb{Z}\cong\mathbb{Z}/ab\mathbb{Z}$

Vediamo che $\mathbb{Z}/n\mathbb{Z}$ è un campo $\iff$ n è primo.

§2 Un pò di teoria di gruppi

Sia $(G, \circ)$ gruppo di ordine n, $H \leq G$ un sottogruppo
spiegare spiegare

Definiamo una relazione su G:
$$a \sim b \quad \text{se} \quad ab^{-1} \in H$$

Come in §1, $\sim$ è una relazione di equivalenza e induce una partizione su G
$$G = \overline{a_1} \cup \dots \cup \overline{a_r}$$
dove $a_1, \dots, a_r \in G$ e $\overline{a_1}, \dots, \overline{a_r}$ sono le classi di equivalenza distinte di G rispetto a $\sim$ (i laterali di G modulo H).

Per ogni $1 \leq i \leq r$
$$\overline{a_i} = \{x \in G \mid x \sim a_i\} = \{ha_i \mid h \in H\} \quad \text{e} \quad |\overline{a_i}| = |H|$$
$\exists h \in H : x = ha_i \iff xa_i^{-1} \in H$

Dunque $n = |G| = \sum_{i=1}^{r} |\overline{a_i}| = r \cdot |H|$.

Abbiamo dimostrato:

Teorema di Lagrange: se G è un gruppo finito e $H \leq G$, allora $|H|$ divide $|G|$.

In particolare, sia $a \in G$ e sia $H = \langle a \rangle = \{a^k \mid k \in \mathbb{Z}\}$
è un sottogruppo: chiuso per $\circ$, contiene 1 e $(a^n)^{-1} = a^{-n}$

(dove
$$a^k = \begin{cases} \underbrace{a \cdot \ldots \cdot a}_{k \text{ volte}} & \text{se } k > 0 \\ 1 & \text{se } k = 0 \\ \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{k \text{ volte}} & \text{se } k < 0 \end{cases}$$
)

Poiché G è finito, esiste $m \in \mathbb{N}$ tale che
$$H = \{1, a, a^2, \dots, a^{m-1}\} \text{ e}$$
$a^k = a^l \Rightarrow a^{k-l} = 1$

m è il minimo intero positivo tale che $a^m = 1$.

Per il Teorema di Lagrange $\underset{|G|}{n} = \underset{|H|}{m} \cdot r$, quindi $a^n = (a^m)^r = 1$.

Dunque si ha

<u>Corollario</u> In un gruppo G di ordine n ogni elemento $a \in G$ soddisfa $a^n = 1$.

Se applichiamo il Corollario a $G = (\mathbb{Z}/n\mathbb{Z}^*, \cdot)$ di ordine $\varphi(n)$ otteniamo

<u>Teorema di Fermat-Eulero</u> Siano $x, n \in \mathbb{N}$ due numeri coprimi. In $\mathbb{Z}/n\mathbb{Z}$ si ha $\overline{x}^{\varphi(n)} = \overline{1}$.

($MCD(x,n) = 1$, dunque $\overline{x} \in \mathbb{Z}/n\mathbb{Z}^*$)

§3 <u>Dimostrazione dell'Algoritmo RSA</u>

$n = pq$, $m = (p-1)(q-1) = \varphi(n)$,

$1 < a < m$ primo con m, $1 < b < m$ con $ab = 1 + \beta m$

Dato $1 < x < \min(p,q)$ siano $y, x' \in \{1, \dots, n-1\}$ tali che in $\mathbb{Z}/n\mathbb{Z}$

$\overline{x}^a = \overline{y}$, $\overline{y}^b = \overline{x}'$.

Si noti che x è primo con n, quindi $\overline{x}^{\varphi(n)} = \overline{1}$. Dunque

$\overline{x}' = \overline{x}^{ab} = \overline{x}^{(1+\beta m)} = \overline{x} \cdot (\overline{x}^{\varphi(n)})^{\beta} = \overline{x}$

e poiché $1 < x, x' < n$, segue $x' = x$.

$\square$

MCD e Algoritmo Euclideo

<u>LEMMA</u> $a = bq + r \Rightarrow MCD(a,b) = MCD(b,r)$

<u>Dim.</u> $d = MCD(b,r)$ divide a, quindi comun divisore di a,b
se t divide a,b, allora t divide anche $a - bq = r$,
quindi comun divisore di b e r e pertanto t divide d.
Dunque d è MCD di a e b.

<u>Algoritmo Euclideo</u> Siano $a,b \in \mathbb{N}$, $a > b$. Se b divide a, allora $b = MCD(a,b)$.
Altrimenti eseguiamo divisioni successive ponendo

$a = b q_1 + r_1$ con $0 < r_1 < b$

$b = r_1 q_2 + r_2$ con $0 \leq r_2 < r_1 < b$

$r_1 = r_2 q_3 + r_3$ con $0 \leq r_3 < r_2 < r_1 < b$

$\vdots$

$r_{n-3} = r_{n-2} q_{n-1} + r_{n-1}$

$r_{n-2} = r_{n-1} q_n + r_n$

$r_{n-1} = r_n q_{n+1} + r_{n+1}$ con $r_{n+1} = 0$

Allora $r_n = MCD(a,b)$ ed esistono $\alpha, \beta \in \mathbb{N}$ tali che

$MCD(a,b) = \alpha a + \beta b$

<u>Dim.</u>

$$MCD(a,b) = MCD(b, r_1) = MCD(r_1, r_2) = MCD(r_2, r_3) = \dots$$
$$= MCD(r_{n-1}, r_n) \underset{\substack{\uparrow \\ r_n \text{ divide } r_{n-1}}}{=} r_n$$

Inoltre $r_n = r_{n-2} - r_{n-1} q_n = r_{n-2} - (r_{n-3} - r_{n-2} q_{n-1}) q_n$ comb. lin. di r_{n-2}, r_{n-3}

$= \dots$ comb lin di r_1, b

$= \dots$ comb. lin. di a, b

<u>COR.</u> (Id. di Bézout) a,b coprimi $\Leftrightarrow \exists \alpha, \beta$ tali che $1 = \alpha a + \beta b$